HP StorageWorks Edge Switch release notes

Part number: Product Number: AA–RTDZG–TE/958–000284–007
(March 2005) Seventh edition:

Legal and notice information

Printed in the U.S.A.

HP StorageWorks Edge Switch release notes

About this document

These release notes contain late breaking and supplemental information for the Edge Switch 2/12, Edge Switch 2/24, and Edge Switch 2/32.

Be sure to read these release notes before installing an edge switch. This information is periodically updated and available on the following HP web site: http://thenew.hp.com/country/us/eng/prodserv/storage.html.

- Release notes information
- Intended audience
- Firmware version 07.00.00-84
- Other edge switch documentation
- CDROM directory structure
- Supported configurations
- Cable requirements
- Important information
- Known issues

Release notes information

These release notes cover the following major topics:

- Certain unauthorized devices may increase response time for fabric operations under specific conditions with the Edge Switch 2/24
- HSG80 transparent mode not supported with IBM AIX
- HSG80 transparent mode not recommended with controller in SCSI-3 mode with
- ISL disconnect causes NOS error with the OpenVMS operating systems
- Support for speed Auto-Negotiate
- Ports may accumulate spurious events
- Possible switch reset after power failure or power off sequence
- SNMP issues

Intended audience

This document is intended for customers who purchased the Edge Switch 2/12, Edge Switch 2/24, and Edge Switch 2/32.

Firmware version 07.00.00-84

Firmware 07.00.00-84 is the latest (as of this date), firmware released with the Edge Switch 2/12, Edge Switch 2/24, and Edge Switch 2/32. A copy of firmware 07.00.00-84, is contained on the *HP StorageWorks edge switch documentation and firmware CD*, (Part Number 524-000001-006). The latest firmware is also available on the following HP web site: http://h18006.www1.hp.com/storage/saninfrastructure.html.

For more information on upgrading firmware versions, refer to the appropriate HP StorageWorks edge switch service manual. The features of this firmware version are detailed in the following manuals.

Other edge switch documentation

In addition to these release notes, HP provides the following corresponding information:

- *HP StorageWorks Edge Switch 2/12 Flexport Upgrade Instructions*, AA-RV14D-TE/958-000339-003
- *HP StorageWorks Edge Switch 2/12 Installation Guide*, AA-RURCC-TE/958-000340-002
- *McDATA Sphereon 4300 Fabric Switch Installation and Service Manual*, 620-000171-010
- *HP StorageWorks Edge Switch 2/24 Flexport Upgrade Instruction*, AA-RTDHF-TE/958-000286-005
- *HP StorageWorks Edge Switch 2/24 Installation Guide*, AA-RTDWC-TE/958-000283-002
- *McDATA Sphereon 4500 Fabric Switch Installation and Service Manual*, 620-000159-320
- *HP StorageWorks Edge Switch Element Manager User Guide*, AA-RS2HD-TE
- *HP StorageWorks Edge Switch 2/32 Flexport Upgrade Instruction*, AA-RS33F-TE/958-000291-004
- *HP StorageWorks Edge Switch 2/32 Installation Guide*, AA-RSTZE-TE/958-000290-003

- *McDATA Sphereon 3232 Fabric Switch Installation and Service Manual*, 620-000155-210
- *McDATA Enterprise Operating System Command Line Interface User Manual*, 620-000134-720
- *McDATA EOS SNMP Support Manual*, 620-000131-620
- *McDATA Products in a SAN Environment Planning Manual*, 620-000124-500
- *HP StorageWorks SAN Design Guide*, AA-RMPNT-TE
- *McDATA SANpilot User Manual*, 620-000160-230
- *HP StorageWorks HA-Fabric Manager User Guide*, AA-RS2CF-TE
- *HP StorageWorks HA-Fabric Manager Transition Guide*, AA-RV1MB-TE
- *HP StorageWorks HA-Fabric Manager Appliance Installation Guide*, AA-RU5FC-TE/958-000324-002
- *HP StorageWorks HA-Fabric Manager Release Notes*, AA-RUR6E-TE/958-000288-009
- *HP StorageWorks Director and Edge Switch Glossary*, AA-RU5JB-TE
- *HP StorageWorks C-FCSWAPI SDK Bridge Agent Installation Instructions*, AA-RVJ1B-TE/958-000405-001

CD-ROM directory structure

The HP StorageWorks edge switch documentation and firmware CD contains the following items:

- `Manuals.pdf`—HP StorageWorks Edge Switch 2/12, Edge Switch 2/24, and Edge Switch 2/32 Documentation; links to the following documents and search function
- Documents
  - `README.TXT`—HP document structure; late-breaking doc changes
  - AA-RV14D-TE/958-000339-003—*HP StorageWorks Edge Switch 2/12 Flexport Upgrade Instructions*
  - AA-RURCC-TE/958-000340-002—*HP StorageWorks Edge Switch 2/12 Installation Guide*
  - 620-000171-010—*McDATA Sphereon 4300 Fabric Switch Installation and Service Manual*
  - AA-RTDWD-TE/958-000283-003—*HP StorageWorks Edge Switch 2/24 Installation Guide*
  - 620-000159-320—*McDATA Sphereon 4500 Fabric Switch Installation and Service Manual*

- AA-RS2HD-TE—*HP StorageWorks Edge Switch Element Manager User Guide*
- AA-RSTZE-TE/958-000290-003—*HP StorageWorks Edge Switch 2/32 Installation Guide*
- 620-000155-210—*McDATA Sphereon 3232 Fabric Switch Installation and Service Manual*
- 620-000134-720—*McDATA Enterprise Operating System Command Line Interface User Manual*
- 620-000131-620—*McDATA EOS SNMP Support Manual*
- 620-000124-500—*McDATA Products in a SAN Environment Planning Manual*
- AA-RMPNT-TE—*HP StorageWorks SAN Design Guide*
- 620-000160-230—*McDATA SANpilot User Manual*
- AA-RU5FC-TE/958-000324-002—*HP StorageWorks HA-Fabric Manager Appliance Installation Guide*
- AA-RS2CF-TE—*HP StorageWorks HA-Fabric Manager User Guide*
- AA-RV1MB-TE—*HP StorageWorks HA-Fabric Manager Transition Guide*
- AA-RU5JB-TE—*HP StorageWorks Director and Edge Switch Glossary*
- AA-RVJ1B-TE/958-000405-001—*HP StorageWorks C-FCSWAPI SDK Bridge Agent Installation Instructions*

- Firmware
  - `HPQ_MSF_v07.00.00-84.bin`—HP StorageWorks M-Series firmware
  - `firmwareupdate.txt`—Instructions for updating firmware
- Acrobat
  - `RP505ENU.EXE`—Windows installation file for Acrobat Reader 5.0 with Search

Supported configurations

Operation of multiple switches in a fabric topology is subject to the following topology limits. Consider the impact of these limits when planning the fabric.

NOTE:

For more information about planning the fabric, refer to *HP StorageWorks SAN High Availability Planning Guide*.

- **Fabric Elements**—Each fabric element is defined by a unique domain ID that ranges between 1 and 31; therefore, the theoretical limit of interconnected directors in a single fabric is 31. The supported limit of interconnected switches in a single fabric is 24. Because this number is subject to change, contact your HP authorized service representative for the current number of interconnected switches supported in a single fabric.
- **Inhomogeneous fabric**—To determine if interoperability is supported for a product, or if restrictions apply, refer to the product publications, or contact your HP authorized service representative.
- **Number of Interswitch Links (ISLs)**—The maximum supported number of ISLs for edge switches is all available switch ports. For redundancy, at least two ISLs should connect any two switch-class fabric elements. Because this number is subject to change, contact your HP authorized service representative for the current number of ISLs supported per switch.
- **Hop Count**—The Fibre Channel theoretical limit of ISL connections traversed (hop count) in a single path through a fabric is seven. The maximum supported hop count in a single path through a fabric is three. Because this number is subject to change, contact your HP authorized service representative for the current hop count supported by a single fabric path.

  The hop count is equal to the number of ISL connections traversed in a single path, not the total number of ISL connections between devices.

Cable requirements

NOTE:

Optical cables for the Edge Switch 2/12, Edge Switch 2/12, and Edge Switch 2/32 must be ordered separately.

For cables measuring up to 500 meters (1 Gbps) or 300 meters (2 Gbps), use multi-mode Fibre Channel cables. For longer cables, use single-mode Fibre Channel cables.

Multi-mode optical cables are connected to short-wave optical transceiver modules in a switch. Single-mode optical cables are connected to long-wave optical transceiver modules in a switch. Multi-mode cables should use 50/125 optical fibers, and single-mode cables typically use 9/125 optical fibers for distances up to 10 km.

Verify that connectors interfacing with the Edge Switch 2/12, Edge Switch 2/24, and Edge Switch 2/32 use LC Duplex connectors with a PC finish. In addition, the connector at the opposite end of the cable must be of either LC or SC type, depending on the requirements of the connected device.

Important information

This section describes important information related to the Edge Switch 2/12, Edge Switch 2/24, and Edge Switch 2/32.

Features not supported in this release

The following director and edge switch feature is not supported in this release:

- SANtegrity Authentication

The following HAFM features are not supported in this release:

- SANtegrity Security Center
- Group Configuration Manager

These features are described in the documentation released with firmware 07.00.00 and HAFM 08.06.00. Some of these features may be available in a future release.

Documentation released with firmware 07.00.00 and HAFM 08.06.00

To support these products, we are providing documentation from both McDATA Corporation (the product developer) and from HP (the product OEM). The HP documents include all information HP has incorporated into the products to date. The McDATA documents include only the basic product information.

Table 1 shows HP terminology and McDATA Corporation equivalents used in the McDATA documents.

Table 1 HP and McDATA terminology

HP term	McDATA term
HP StorageWorks Edge Switch 2/12	Sphereon 4300 Fabric Switch
HP StorageWorks Edge Switch 2/16	Sphereon 3216 Fabric Switch
HP StorageWorks Edge Switch 2/24	Sphereon 4500 Fabric Switch
HP StorageWorks Edge Switch 2/32	Sphereon 3232 Fabric Switch
HP StorageWorks Director 2/64	Intrepid 6064 Director
HP StorageWorks Director 2/140	Intrepid 6140 Director
Embedded Web Server (EWS)	SANpilot
HA-Fabric Manager (HAFM)	Enterprise Connectivity Manager (EFCM)
Firmware	Enterprise Operating System (E/OS)
HAFM Appliance	EFC Server

HAFM and firmware compatibility

Table 2 lists the minimum version of HAFM that can run with the various versions of firmware for the directors and edge switches.

Table 2 HAFM and firmware compatibility

Firmware version	HAFM version (minimum)
01.01.02	04.00.01 (HP EFCM)
01.02.02-06	04.01.02-14 (SDCM)
01.03.00-35	04.02.00-40 (HP EFCM)
01.04.00-01	04.02.00-40 (SDCM)
02.00.00-33	06.00.00-45 (HP EFCM)
02.00.02-01	06.00.02-06
04.01.02-04	06.03.01-05
05.02.00-13	07.01.00-09 (Notebook Server)
05.02.00-13	07.02.00-09 (HAFM Appliance)
05.05.00-12	None (Edge Switch 2/12)
06.01.00-18	07.01.00-09 (Notebook Server)
06.01.00-18	07.02.00-09 (HAFM Appliance)
06.01.00-18	08.02.00 recommended (HAFM Appliance)
06.02.00-22	07.01.00-09 (Notebook Server)
06.02.00-22	07.02.00-09 (HAFM Appliance)
06.02.00-22	08.02.00 recommended (HAFM Appliance)
07.00.00-84	07.01.00-09 (Notebook Server)
07.00.00-84	07.02.00-09 (HAFM Appliance)
07.00.00-84	08.06.00 recommended (HAFM Appliance)

Prerequisites for installing and using firmware 07.00.00

If you are using HAFM, firmware 07.00.00 requires HAFM 07.01.00 or later (check with HP Customer Support for the latest shipping version of HAFM). HAFM should be at the minimum level before installing the new firmware.

NOTE:

HAFM is not required for operating hardware products using the firmware.

All directors and edge switches in the same fabric should have the same firmware level installed. Although products may co-exist in a fabric running different levels of firmware, all products *must* be at the same major functional release level.

Upgrading from an earlier version of firmware

Upgrading to firmware 07.00.00-84 is non-disruptive to attached devices. The director or edge switch is not required to be offline before performing an upgrade operation. Limitations to upgrades are clearly identified if there are any limitations to performing the operation.

Before upgrading firmware, it is highly recommended that you back up the director or edge switch configuration. Refer to your *HP StorageWorks Edge Switch Element Manager User Guide* for more information. Embedded Web Server (EWS) also provides an option to print or save product configuration to a file. Refer to the *HP StorageWorks Embedded Web Server User Guide* for more information.

All products must be running firmware 06.00.00 or later before upgrading to 07.00.00-84. If a switch is operating with a firmware level earlier than 06.00.00, you must upgrade to 06.xx.xx before installing 07.00.00-84.

Upgrades and downgrades are supported only from one major release to the next, such as from 06.xx.xx to 07.00.00-84. If EWS is used for upgrades and downgrades, and this rule is not followed, errors occur and there may be a disruption to attached devices.

If upgrading to firmware 06.02.00-22 requires you to upgrade from 04.xx.xx to 05.xx.xx in the process, there are special considerations, as detailed in the section, Upgrading firmware on an edge switch from 04.xx.xx to 05.xx.xx.

A small number of early-shipped Surestore Director FC-64 units may receive one of the following messages when they upgrade to firmware 05.02.00-13:

- HAFM—`Firmware cannot be loaded due to insufficient CTP memory.`
- EWS—`File System Error:  Insufficient memory for new firmware version.`

This occurs only in certain units with CTP cards. Units with CTP2 cards do not have this issue.

If you get one of these messages during the upgrade, the firmware upgrade failed, but the unit continues working with the existing firmware without an interruption in service. The upgrade process checks for sufficient memory before activating the new firmware image. The firmware upgrade does not complete without sufficient memory. Please contact HP Customer Support if you receive this message.

Upgrading firmware on an edge switch from 04.xx.xx to 05.xx.xx

An issue has been identified in release 04.xx.xx if the contents of the nonvolatile storage (NVRAM) on the CTP become corrupted. Once the configuration has been loaded, this corruption is not detected until an IPL/IML, power cycle, or firmware code load. If the NVRAM in the CTP has corrupted contents, the firmware load can cause the configuration to reset to factory defaults, which could cause a system outage.

Edge switch products already running 05.01.00 or later continually validate the NVRAM configuration, so risk of an outage is extremely low. For edge switch products running an earlier version of firmware, the risk of an outage increases due to the NVRAM issue. If an outage compromises system integrity, HP recommends that the edge switch firmware upgrade be a scheduled maintenance action that anticipates the failure of switch connectivity. This issue was corrected with firmware 05.02.00-13 and later.

To safely upgrade firmware on a edge switch, perform the following:

1. Upgrade HAFM software on the HAFM server/appliance to 07.01.00 (minimum).
2. Download firmware 05.02.00-13 using the **Firmware Library** option under the Product Manager Maintenance menu.
3. Back up the edge switch configuration using the **Backup & Restore Configuration** option under the Product Manager Maintenance menu.
4. Upgrade the firmware to 05.02.00-13 on each edge switch using the **Send** option on the Firmware Library dialog box.

Considerations for downgrading the version of firmware

Directors or edge switches are not required to be offline before performing a firmware downgrade operation. Limitations to downgrades are clearly identified if there are any limitations to performing the operation.

Before downgrading firmware, it is highly recommended that you back up the director or edge switch configuration. Refer to your *HP StorageWorks Edge Switch Element Manager User Guide* for more information. EWS also provides an option to print or save product configuration to a file. Refer to your *HP StorageWorks Embedded Web Server User Guide* for more information.

Before downgrading below 07.00.00-84, there can only be one user assigned access rights as Administrator and one user assigned as Operator for Embedded Web Server and CLI. If additional users were created, you have to delete them before downgrading. Firmware 07.00.00-84 does not allow the last user with Administrator rights in Embedded Web Server or CLI to be deleted. If no Operator user exists, firmware 07.00.00-84 automatically creates one for each interface during the downgrade. If more than one Administrator and/or one Operator exists for Embedded Web Server and/or CLI, when attempting to downgrade you are prompted to delete one of them first.

When downgrading to a release prior to 07.00.00-84, any modifications to the port RX BB_Credit settings using the new enhanced port configuration capability must be changed back to a configuration supported by older firmware. This is necessary to allow the configuration to comply with previous releases' configuration database. Firmware 07.00.00-84 services verify compatibility and prevent downloads until the configuration conflict is resolved.

For procedures to download firmware to the switch or director using the HAFM Element Manager interface or EWS interface, refer to the following:

- The switch or director Installation and Service Manual. This publication provides complete procedures for obtaining firmware from the HP web site and downloading firmware to the switch or director using HAFM.
- The switch or director Element Manager online help and User Manual. These includes instructions for downloading firmware to the switch or director using the HAFM interface.
- EWS User Manual. This provides procedures for downloading firmware to the switch or director.
- EWS online help. This provides procedures for downloading firmware to the switch or director.

Downgrading directly to a release before 06.00.00 from 07.00.00-84 is not allowed. To downgrade to a release before 06.00.00, you must first downgrade to 06.YY.ZZ.

Upgrades and downgrades are supported only from one major release to the next, such as from 06.xx.xx to 07.00.00-84. If EWS is used for upgrades and downgrades, and this rule is not followed, errors occur and there may be a disruption to attached devices.

Downgrading to release 6.0 with the Preferred Path feature configured could cause loss of this function. HP recommends that Preferred Path be disabled before downgrading. To do this, deselect the check box for **Enable Preferred Path** in the Configure Preferred Paths dialog box.

NOTE:

The Director 2/140 and the Edge Switch 2/24 cannot be downgraded earlier than 04.01.00, and the Edge Switch 2/12 cannot be downgraded earlier than 05.05.00.

Downgrades directly to 05.03.01 from 06.xx.xx is not concurrent when the second-generation Edge Switch 2/24 is configured in **Open Fabric** operating mode. In other words, downgrades in **Open Fabric** mode cannot be done with the second-generation Edge Switch 2/24 online without disrupting port operations. Since second-generation Edge Switch 2/24 switches cannot be downgraded earlier than 05.03.01, they must be configured in **Homogeneous Fabric Interoperability** mode to remain concurrent. If this process is not followed, I/O through the switch may be significantly disrupted or stopped. Recovery for this situation is accomplished by reactivating the current zone set.

If you are installing a new or replacement second-generation Edge Switch 2/12 or Edge Switch 2/24 into an existing 05.xx.xx fabric, HP recommends that you downgrade the unit before installing it into the fabric.

Downgrading to 05.05.00 is supported only on first-generation Edge Switch 2/12 switches. Second-generation Edge Switch 2/12 switches can be downgraded only to 05.05.01. Second-generation Edge Switch 2/24 switches can be downgraded only to 05.03.01.

If a Director 2/140 in a multiswitch fabric is downgraded earlier than 06.02.00, ISLs could become segmented if there are any other switches in the fabric operating with a firmware version earlier than 06.01.00. To prevent this situation, downgrade all Director 2/140s in the fabric to 06.01.00 before downgrading any products in the fabric to 05.xx.xx. This problem only exists with Director 2/140s in the fabric. HAFM displays a warning message if a downgrade from 06.02.00 is attempted, but you can continue with the downgrade if desired.

NOTE:

The warning message is displayed when downgrading any model from 06.02.00, but only applies to downgrade operations for the Director 2/140.

Firmware downgrades should not be performed using EWS and Internet Explorer v5.00.3315.1000x. If this operation is performed, the download operation may not complete and may eventually time-out leaving the switch with the previous version of firmware.

HAFM upgrade required for firmware version 07.xx.xx

To upgrade to firmware 07.00.00-84, you must first upgrade the HAFM software to 07.01.00-9 minimum, if you are using the notebook HAFM server to manage the director or edge switch. The HAFM software is contained on the HP StorageWorks ha-fabric manager documentation and software CD (Part Number 516-000024-820). An upgrade kit to HAFM 07.01.00-9 is also available, Part Number 320908-B22, for owners of license for previous versions. This HAFM upgrade is also available on the following HP web site: http://h18006.www1.hp.com/storage/saninfrastructure.html

If you are using the 1U rack-mount HAFM appliance to manage the director or edge switch, the minimum HAFM version required is 07.02.00-9, which is the minimum version installed. This HAFM software is contained on the HP StorageWorks ha-fabric manager documentation and software CD (Part Number 516-000024-720).

The previous minimum versions of HAFM allow you to manage directors or edge switches running 07.00.00-84 firmware, but to be able to use all the new features and enhancements, you need to upgrade HAFM to 08.06.00, which runs only on the 1U rack-mount HAFM appliance.

As an alternative, you can perform the firmware upgrade directly to the director or edge switch using their EWS.

Please contact your local HP technical resource if you need to obtain a new HAFM version.

Please contact your local HP technical resource to confirm compatibility with devices in your SAN before upgrading to this firmware version.

For more information on upgrading software versions, refer to the *HP StorageWorks HA-Fabric Manager User Guide.* The features of this software version are detailed in the accompanying manuals listed in section Other edge switch documentation.

Zone FlexPar feature

Because zoning is managed on a fabric-wide basis, all switches and directors in the fabric must maintain the same zoning configuration. This configuration is maintained automatically through the Fibre Channel protocol.

To keep this information current, RSCN messages are sent through the fabric to inform attached devices when zoning changes occur, when devices become available, or when devices become unavailable. In the case where devices become available or unavailable, RSCNs are sent only to the devices in the same zone. Zoning changes, however, trigger RSCNs to be sent to all of the devices in the fabric. As fabrics grow larger and larger, the quantity of RSCNs from zoning changes can create congestion and disrupt devices, causing them to pause normal activity to determine the status of the other devices. This can occur even if the new device is not zoned to talk to the other devices in the fabric.

With the Zone FlexPar feature enabled, RSCN messages for a zoning change are handled like RSCNs for availability/unavailability changes. Specifically, RSCNs are restricted to only those devices sharing at least one common zone with the device that changed. This way, only devices that are impacted by the change in connectivity receive RSCNs.

The Zone FlexPar feature is available in both Open Fabric 1.0 and Homogeneous Fabric 1.0 Interop modes, as well as in environments with loop-attached devices. In Homogeneous Fabric 1.0 mode, the default zone is treated like any other zone, and RSCNs are sent only to the affected devices if the default zone is enabled or disabled. A PFE key is not required for the Zone FlexPar feature, and it can be enabled or disabled through CLI for a specific switch. When upgrading to firmware 07.00.00 or installing a new switch with firmware 07.00.00 the feature is enabled by default, allowing it to work immediately. If the Zone FlexPar feature is not enabled on all switches in the fabric, the restricted RSCN distribution only applies for devices attached to switches with the feature enabled.

Enhanced SANtegrity Security Suite

SANtegrity Security Suite enhanced features include authentication support for device login, interswitch connections and management interfaces. The Secure Access features are included as a standard part of the SANtegrity Security Suite in firmware 07.00.00.

Standard features

The following SANtegrity features do not require a license or SANtegrity Binding.

- **CHAP Authentication for HAFM/SWAPI**—This provides authentication of connections from the HAFM appliance service processor and SWAPI Direct Connect. This ensures that requested HAFM management sessions or SWAPI Direct Connect sessions are from a trusted source.

- **Encryption of Passwords and Secrets Shared with HAFM**—All secrets and password information are passed in encrypted format for greater security. This prevents "snooping" of Ethernet connection to capture user login and authentication secret information.
- **RADIUS Server Support**—This provides support for IETF RADIUS (Remote Authentication Dial In User Service) protocol for password authentication. Firmware 07.00.00 allows users to configure settings for using a RADIUS server. RADIUS provides centralized authentication services for multiple devices on a network. This means that several switches can be configured to use a single RADIUS server.
- **Prompted Change of EWS and CLI Passwords from Default**—This prompts users to modify the password settings for both the CLI and EWS interfaces the first time they log in using either of these interfaces.
- **RBAC Phase I: Enhanced User Rights Configuration**—RBAC is role based access control. This is the first phase of more comprehensive role-based access control planned for the CLI and EWS interfaces. Multiple users can now be configured for EWS or CLI, or both, through either interface. This allows users to configure additional user name/password combinations.
- **SSH for CLI**—Secure Shell (SSH) provides an encrypted connection, as an alternative to Telnet, to secure CLI access to switches and directors.
- **Enhanced Maintenance Port Security**—This allows users to enable enhanced authorization on the maintenance port, which is the switch or director RS-232 connection. Enhanced Authorization mode enforces stronger security policies, requiring users to change the well-known password to a case- sensitive private password the first time they use the maintenance port. Subsequent access by service personnel will require log in through the private customer-level access.
- **Security Log**—The Security Log is a new log available in EWS, CLI, and HAFM that records various events concerning integrity of a switch. This includes authorization or authentication problem detection, and approved and invalid access attempts. Each log entry provides an event number or reason, a date/time stamp, a trigger level (a type of security event severity), an event count, and a category and data pertaining to the specific event. The log wraps at 200 entries. This log provides customers with details to track down attempted security threats and identify the source of problems that might jeopardize the switch integrity.
- **IP Access Control List**—This allows users to establish a list of IP addresses from which the switch is allowed to accept connections. This prevents users who have access to the Ethernet LAN from attempting to access the Fibre Channel switches. Connection attempts from unauthorized IP addresses are ignored by the switch, making it appear that no device is connected. This is primarily intended for environments that are not on a private, inaccessible subnet, such as when installed in most cabinet configurations with a dual-NIC HAFM appliance Processor.

Advanced Fabric Diagnostics

This provides tools to monitor the fabric and identify potential problems before they impact network and application performance. Tools include ISL Fencing, new switch-centric Fabric and Embedded Port Logs, an Audit Log for the embedded user interfaces, and access to the Digital Diagnostic capabilities included with newer SFP transceivers.

ISL fencing

Also called Port Fencing, this feature allows customers to set up policies for blocking an ISL when problems occur that cause an ISL to "bounce" or repeatedly attempt to establish a connection. Any time an ISL is brought up or down, a fabric rebuild occurs, which can cause disruption in some environments. ISL Fencing will lessen the likelihood of having a problematic ISL connection disrupt a SAN.

To configure this feature, users set policies with thresholds based on the number of port events occurring during a set time period. If a port generates enough events to exceed the policy threshold, the port is automatically blocked and the user is notified. Transmit and receive traffic is disabled until the user can investigate, solve the problem, and manually unblock the port.

Embedded Audit Log

The Audit log is a new log available through CLI and EWS. This is not the same Audit Log available through HAFM. The log records all configuration changes to the switch to provide data for analyzing problems caused by configuration changes.

Embedded Port Log

The Embedded Port Log is a new log that records all Fibre Channel traffic from or to the embedded port. This log is actually implemented as two logs, one that allows entry wrapping and one that stops adding entries when filled. The logs allow filtering based on Class F frames, as well as by port number, to isolate specific events or problems.

This feature is intended for advanced users to diagnose and troubleshoot traffic problems within a SAN. The Embedded Port Log is available via EWS, CLI, and HAFM.

Embedded Fabric Log

The switch-based fabric log records events related to the following services:

- Fabric Controller
- Path Selection
- Login Server
- Name Server

The Fabric log is actually implemented as two logs, one that allows entry wrapping and one that stops adding entries when filled. This log is intended to provide information for analyzing fabric and switch behaviors and problems. The Fabric log is available via EWS, CLI, and HAFM.

OSMS change

Open Systems Management Server (OSMS) is now available as a standard feature. OSMS can be enabled/disabled via EWS, Command Line Interface (CLI), and HAFM.

Default zone is disabled by default

The default zone on the Edge Switch 2/12, Edge Switch 2/24, and Edge Switch 2/32 is disabled by default. Zoning must be configured in order for any devices connected to the edge switches to communicate.

Some IP addresses must be avoided

If you use HAFM to manage other M-Series Fabric directors and edge switches, when you select IP addresses for edge switches, directors, and for the HAFM appliance, do not use IP addresses in the following range:

192.168.0.0 through 192.168.0.255—This subnet is used internally to the HAFM appliance. Using an IP address in this range causes the call-home feature to function incorrectly.

Hard zoning

Hard zoning is a security enhancement introduced in firmware 05.01.00-24 that prevents ports from accessing devices outside their zones. Hard zoning is enabled by default when using firmware 05.01.00-24 or greater and cannot be disabled. All HP-approved host bus adapters (HBAs) limit access to devices within their zones, so you will not see a change in fabric behavior unless you are using nonstandard HBAs. Hard zoning improves security against intruders that load nonstandard HBA drivers.

Hard zoning is compatible with legacy zone definitions, including World Wide Name (WWN) and port zoning. You can use your existing zones and zone sets without any changes. There are no changes to the zoning interfaces, so you do not need to modify your zone management practice, modify your documentation, or retrain Storage Area Network (SAN) administrators.

Hard zoning controls access at the ingress port. When a port attempts to send a frame to a destination outside its zones, the frame is blocked. A Class 2 frame is fabric rejected, and a Class 3 frame is dropped.

Zoning change RSCN control

Normally, when a zone set is activated, a fabric format domain Register State Change Notification (RSCN) is sent to all devices in the fabric. With firmware 05.00.00 or later, you can disable these RSCNs from being sent. This is done using the **Suppress RSCNs on zone set activations** check box on the Configure Switch Parameters dialog box.

This feature significantly changes the normal behavior of the fabric. Devices will have no warning when zones change and will not automatically update their zoning information. The ability to suppress RSCNs is disabled (check box is not selected) by default. This feature can be configured through HAFM, EWS, and CLI.

SNMP changes

Firmware 07.00.00-84 supports the following management information base (MIB) versions on all products:

- Fabric Element MIB: 1.1
- MIB-II MIB: RFC-1213, non-implemented sections are not included
- FCEOS MIB: 2.0
- SNMP Framework MIB: RFC-2271 (1997/09/30)
- FA MIB: 3.0
- FA MIB: 3.1

SNMP requests can be received in either 3.0 or 3.1 of the Fibre Alliance (FA) MIB, and the switch responds in the same version. The switch can also be configured to use a specific version for traps generated by the switch.

Zoning limitations

With firmware 06.00.00 and later, you have the ability to configure large zone sets, including up to 1024 zones and 1024 end ports in a single zone set. Table 3 shows the supported limits for the edge switches and directors.

Table 3 Zoning parameters supported limits

Zoning parameter	Maximum value
Number of zone members in a zone	2048
Number of zones in a zone set	1024
Number of unique zone members in a zone set	2048
Total number of zone members in a zone set (where a zone member can be in multiple zones)	4096
Characters per zoning name	32
Number of unique zone members in HAFM Zoning Library	2048
Number of zones in HAFM Zoning Library	1024
Number of zone sets in HAFM Zoning Library	64
Number of end ports	1024
Number of devices supported (including loop devices)	1024

Using the same firmware

All directors and edge switches in the same fabric should have the same firmware level installed—whether 1 Gbps or 2 Gbps capable, this firmware operates correctly.

The recently released Edge Switch 2/12 had an interim firmware specific for the Edge Switch 2/12, 05.05.00-12. This firmware cannot be used for any other edge switch or director. This interim version is compatible with the M-Series firmware 05.02.00-13 used for the rest of the M-Series fabric products. The firmware 07.00.00-84 is a common firmware for all the M-Series fabric products, including the Edge Switch 2/12.

Firmware 06.02.00-22 provides support for second-generation Edge Switch 2/12 and Edge Switch 2/24 switches. This is the minimum M-Series firmware supported on the second-generation Edge Switch 2/12 and Edge Switch 2/24.

For customers who want to add a second-generation switch to their existing SAN, but are not ready to upgrade their SAN from 5.x to 06.02.00, there is a downgrade firmware version for each of these edge switches which provides compatibility with a SAN running 05.02.00.

Firmware 05.03.01-01 is available for the Edge Switch 2/24, and firmware 05.05.01-01 is available for the Edge Switch 2/12. These versions are installed only on the Edge Switch 2/24 and Edge Switch 2/12, and only when these switches are placed in a M-Series SAN running 05.02.00 firmware. A copy of these versions of firmware, are contained on the HP StorageWorks edge switch documentation and firmware CD (Part Number 524-000001-005).

Reinstalling feature licenses

Feature licenses (or keys) must be reinstalled after performing a factory reset on a director to regain use of the licensed features (e.g., SANtegrity Binding).

Disconnecting the null modem cable

Always log out and disconnect the null modem cable from the serial maintenance port when not in use or when the switch is reset.

CTP controls port lights

Port lights on the edge switch and director products are controlled by the CTP functionality. Certain activities such as firmware updates, IPLing the CTP, or switching over to the backup CTP (director) can cause these port lights to extinguish momentarily until control is reasserted by the CTP. The actual Fibre Channel traffic is not affected during these times.

Ethernet switch support

With firmware 06.00.00 and later, customers can now connect the management port on edge switches and directors to Ethernet switches or hubs. Prior to firmware 06.00.00, only connections to Ethernet hubs were qualified and supported.

Full Volatility

Full Volatility is an optional feature of firmware 06.00.00 and later that is enabled with a feature key. The Full Volatility feature is designed to support high-security environments, which require that customer data not be retained by the edge switch or director after power off.

The feature configures a switch or director so that no frame data is stored after a power off. Without Full Volatility, if the switch or director experiences a fault condition, a dump of the embedded memory space is captured into nonvolatile memory. This dump retains the last 30 frames transmitted from and last four frames transmitted to the embedded port. With Full Volatility installed, this dump does not occur when a fault condition occurs. Although this limits the amount of diagnostic information available for potential problem resolution, the vast majority of problems are typically resolved without the dump files.

Contact your sales representative to purchase a feature key for Full Volatility.

CLI threshold alerts

With firmware 06.00.00 and later, the CLI allows you to set and monitor Throughput Threshold Alerts (TTAs).

CLI show.eventLog command

With firmware 06.00.00 and later, the CLI `show.eventLog` command has been enhanced. The command now displays a Link Incident log and Event log.

MIHPTO value

With firmware 06.00.00 and later, the internal Missing Interrupt Handler Primary Time Out (MIHPTO) value has been changed from 15 seconds to 3 minutes.

EWS enhancements

With firmware 06.00.00 and later, EWS enhancements include support for managing the SANtegrity Binding feature and Enterprise Fabric mode, and providing the Link Incident log and the Open Trunking log.

Preferred Path support

With firmware 07.00.00 and later, this allows users who are not using HAFM to configure preferred data paths through the EWS interface. A preferred path is an ISL data path between multiple fabric elements (directors and switches) that users can configure using the source and exit ports of the origination fabric element, and the domain ID of the destination fabric element.

Configuration Backup

With firmware 07.00.00 and later, this allows users to save switch configuration settings to a standard XML format file, compatible with both HAFM and the Configuration Backup and Restore (CBR) utility. Customers can easily save configuration settings when switch configuration is accidentally modified or at hardware failure. A restore function is not yet available in EWS, but is planned for a future release. In the interim, you can use the complimentary CBR utility to restore configurations settings.

BB_Credit Allocation for ports

Firmware 07.00.00 supports the ability to allocate a specific number of buffer credits per port. This feature provides benefit primarily in the Edge Switch 2/12 and 2/24 switches, where a single pool of buffers is shared among all ports. Users will now be able to allocate buffer credits only where needed. For the Director 2/64, Director 2/140, and Edge Switch 2/32 switches, this enhancement simply allows more granular configuration options for users who want complete configuration control.

NVRAM caching

All writes to non-volatile memory random access memory (NVRAM), which stores configuration data, are now cached to prevent possible corruption of information. Prior to firmware 07.00.00, a small window existed where a switch power-down during an NVRAM write could enable the configuration default settings when the switch is powered back on. All switches and directors are now protected from potential interruptions to NVRAM updates.

Robust large fabrics

Numerous low-level enhancements and optimizations have been made to improve the stability of directors and switches in fabrics containing high populations of devices.

Changing password in CLI

When users are prompted to change the password when logging into the Command Line Interface (CLI), they can enter the default password (password). This will be accepted, however at the next login they will again be required to change the password if it is still the default password.

When users enter the default password when prompted to change the password, new `Security Log entry 10203, Default Password Not Changed`, is posted.

Zoning enhancement to reduce fabric congestion

In Homogeneous Fabric mode, an enhancement was added to reduce unnecessary fabric congestion when performing fabric-wide zoning operations that impact the Default Zone. This enhancement limits the number of members allowed in the Default Zone to 64. When the firmware detects a zoning operation that would cause the member count in the Default Zone to exceed 64 (such as deactivating an active zone set that has more than 64 members), the operation is aborted and the user interface (HAFM 8.6 or EWS) displays the following message: `Zoning request denied: Operation will cause the Default Zone to exceed its limit of 64 members.`

NOTE:

This limit is disabled when the switch parameter **Suppress Zoning RSCNs on Zone set activations** check box is enabled.

Full-fabric capability for Edge Switch 2/12

Unlike other edge switch and director products, a product feature enablement (PFE) key, controls Edge Switch 2/12 E_Port-to-E_Port connections. Once the feature key is purchased and installed, the switch can be configured for E_Port connections on any of the active ports.

The feature key includes distance support. With firmware 06.00.00 and later, the Edge Switch 2/12 ships standard with five buffer-to-buffer (BB) credits allocated to each port. After activation of the Full Fabric feature on a switch, every port has 12 BB Credits allocated to support up to 12 km links at 2Gb/s speeds.

Hard zoning for Edge Switch 2/12 and Edge Switch 2/24 switch loop ports

Firmware 06.00.00 and later extends Hard Zoning to loop (FL) ports on Edge Switch 2/12 and Edge Switch 2/24. Previously, zoning on FL ports was regulated in software.

Known issues

This section describes the known issues related to the Edge Switch 2/12, Edge Switch 2/24, and Edge Switch 2/32.

Certain unauthorized devices may increase response time for fabric operations under specific conditions with the Edge Switch 2/24

When **Port Binding** is enabled, unauthorized devices (devices that are not set up by the **Port Binding**) with older technology can transmit numerous fabric login (FLOGI) requests, which are rejected by the Edge Switch 2/24. Processing these exchanges may increase fabric response times for activities such as fabric builds and valid FLOGI response time for other ports.

Workaround

Remove the unauthorized device, change the **Port Binding WWN** (if this device should be authorized), or alternatively, disable **Port Binding**.

HSG80 transparent mode not supported with IBM AIX

Use of an HSG80 with IBM AIX is restricted to operating the HSG80 in Multibus mode with the Edge Switch 2/12, Edge Switch 2/24, and Edge Switch 2/32. Transparent mode is not supported at this time.

Workaround

None.

HSG80 transparent mode not recommended with controller in SCSI-3 mode with HP-UX operating systems

Due to an issue with nonexistent duplicate LUNs being displayed with the HP-UX operating systems, the HSG80 controller is restricted to SCSI-2 mode of operation when set to Transparent failover mode.

SCSI-3 mode of operation in Multibus failover mode is fully supported with the use of Secure Path software, 3.0 or later versions.

Workaround

None.

ISL disconnect causes NOS error with the OpenVMS operating systems

When an ISL connection is physically removed between directors or switches, the Fibre Channel Adapter model FCA2354 transmits a Not Operational Sequence (NOS) error. This is observed as an entry in the HAFM appliance Link Incident log for the port in which the FCA2354 is attached. The director's Hardware View also displays a yellow triangle icon over the port that detected this incident. The fabric operation or data movement is not disrupted by these incidents, and you can clear alerts from these incidences using the following procedure.

Workaround

Use these steps to clear the incident alerts.

1. At the **HAFM Hardware View**, click the port module to open the **Port Card View**.
2. Right-click on the port with the yellow triangle icon, and choose **Clear Link Incident Alert(s)**.

Support for speed Auto-Negotiate

Auto-negotiate is supported. However, HP recommends that the port speed for E_Ports (for Interswitch Links, or ISLs) be set to a specific port speed (**1Gb/sec** or **2Gb/sec**, as appropriate for the speed of the directors or edge switches being connected) instead of to **Negotiate**. Using a specific port speed decreases the time for a fabric build in response to some perturbation event in the fabric. Similarly, setting a specific port speed for N_Ports also decreases fabric build time. However, setting a specific port speed for N_Ports is not required.

There are a few older HBA devices that do not always succeed in logging in to a switch port when the port speed is set for auto-negotiate.

Workaround

If an older HBA has difficulty logging into a switch port that has its port speed configured as **Negotiate**, configure that port speed to **1Gb/sec** or **2Gb/sec** according to the operation speed of the HBA connected to that port.

Ports may accumulate spurious events

A port may accumulate *Invalid transmission word* and *Bit-Error Threshold Link Incident* events when a transceiver is poorly seated, resulting in a poor ground connection.

Workaround

Reseating the optical transceiver corrects the problem.

Possible switch reset after power failure or power off sequence

In extremely rare instances, after a power failure or power off sequence, an edge switch or director configuration may be reset to factory default settings. This is evident when HAFM is unable to communicate with the edge switch or director after being powered on. This condition occurs because the IP address assigned to the edge switch or director has been reset to the factory default value (10.1.1.10).

Workaround

If this condition occurs, the configuration of the edge switch or director must be restored, and the IP address must be restored. Also, all licensed features need to be reactivated by entering the license keys again.

SNMP issues

SNMP traps `warmStart` and `coldStart` are not always received across Ethernet switches.

Workaround

None.